ASA 8.X：AnyConnect の Start Before Logon 機能の設定

内容

概要

Start Before Logon(SBL)が有効になっている場合、Windows®のログオンダイアログボックスが表示される前に、AnyConnect GUIのログオンダイアログが表示されます。これによって、VPN 接続が最初に確立されます。Start Before Logon は Windows プラットフォームでのみ使用可能であり、管理者がログイン スクリプトの使用、パスワード キャッシング、ネットワーク ドライブからローカル ドライブへのマッピングなどを制御できるようにします。SBL 機能を使用すると、ログイン シーケンスの一部として VPN をアクティブにできます。SBL はデフォルトでは無効になっています。

AnyConnect VPN クライアント機能の設定の詳細については、『AnyConnect クライアント機能の設定』を参照してください。

注：AnyConnectクライアントでは、SBLに対して行う唯一の設定は、機能を有効にすることです。ログイン前に実施されるこのプロセスは、ネットワーク管理者が自身の状況の要件に基づいて処理します。ログイン スクリプトは、ドメインまたは個々のユーザに割り当てることができます。一般に、ドメインの管理者は、バッチ ファイルまたは類似のものを Active Directory のユーザまたはグループに定義しています。ユーザがログインするとすぐに、ログイン スクリプトが実行されます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 8.x を実行する Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco AnyConnect VPN バージョン 2.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

SBL の重要な点として、PC にログインする前にリモート コンピュータを企業インフラストラクチャに接続することがあります。たとえば物理的な企業ネットワークの外部にいるユーザは、PC を企業ネットワークに接続するまでは企業内リソースにアクセスできません。SBL が有効になっていれば、ユーザに対して Microsoft ログイン ウィンドウが表示される前に AnyConnect クライアントが接続します。Microsoft ログイン ウィンドウが表示されたら、ユーザは通常の方法で Windows にログインする必要があります。

SBL を利用する理由には次のようなものがあります。

- ユーザの PC が Active Directory インフラストラクチャに接続している。
- ユーザの PC にキャッシュされた資格情報を保持できない。つまり、グループ ポリシーでキャッシュされた資格情報が許可されていない。
- ネットワーク リソースから、またはネットワーク リソースへのアクセスを必要とする場所からログイン スクリプトを実行する必要がある。
- ネットワークでマッピングされるドライブを使用し、Active Directory インフラストラクチャの認証を必要とする。
- ネットワーキング コンポーネント（MS NAP/CS NAC など）がインフラストラクチャとの接続を必要とすることがある。

SBL はローカルの社内 LAN への組み込みと等価のネットワークを作成します。SBL が有効な状態では、ユーザがローカル インフラストラクチャにアクセスできることから、オフィス内のユーザのために通常実行されるログイン スクリプトをリモート ユーザにも使用できます。

ログイン スクリプトの作成方法については、Microsoft TechNet の記事 を参照してください。

Windows XP でのローカル ログオン スクリプトの使用方法については、この Microsoft のサポート技術情報 を参照してください。

もう 1 つの例として、キャッシュされた資格情報を PC へのログオンに使用できないようにシステムを設定できます。このシナリオでは、ユーザは社内ネットワーク上のドメイン コントローラと通信できる状態であり、PC へのアクセス前にユーザの資格情報を検証されるようにする必要があります。SBL は、呼び出されたときにネットワークに接続されている必要があります。ワイヤレス インフラストラクチャへの接続のためのユーザ資格情報に基づいてワイヤレス接続が行われることがあるために、場合によってはネットワークに接続できないことがあります。SBL モードがログインのクレデンシャル フェーズに先行するため、このシナリオでは接続できません。このケースで SBL を機能させるには、ログインを通して資格情報をキャッシュするようにワイヤレス接続を設定するか、もしくはその他のワイヤレス認証を設定する必要があります。

Start Before Logon コンポーネントのインストール（Windows のみ）

Start Before Logon コンポーネントは、コア クライアントのインストール後にインストールする必要があります。また AnyConnect 2.2 の Start Before Logon コンポーネントの場合は、バージョン 2.2 以降のコア AnyConnect クライアント ソフトウェアのインストールが必要です。MSI ファイルを使用して AnyConnect クライアントと Start Before Logon コンポーネントを事前に展開する場合（Altiris、Active Directory または SMS など独自のソフトウェア展開手段を持つ大企業の場合など）、正しい順序でインストールする必要があります。AnyConnect が Web 展開または Web 更新されている場合（または両方の場合）、インストールの順序は、管理者が AnyConnect をロードした時点で自動的に処理されます。インストールの詳細については、『リリース ノート：Cisco AnyConnect VPN Client リリース 2.2』を参照してください。

Windows Vista、Windows 7、および Vista 以前のシステムの Start Before Logon との相違点

Windows Vista システムと Windows 7 システムでは SBL を有効にする手順が多少異なります。Vista より古いシステムでは、バーチャル プライベート ダイヤルアップ ネットワーク グラフィカル識別認証（VPNGINA）という名称のコンポーネントで SBL をインストールしていました。Vista および Windows 7 システムでは SBL の実装には PLAP という名称のコンポーネントが使用されます。

AnyConnect クライアントでは、Windows Vista の Start Before Logon 機能は Pre-Login Access Provider（PLAP）と呼ばれています。これは接続可能な資格情報プロバイダーです。この機能を使用すると、ネットワーク管理者は、資格情報の収集やネットワーク リソースへの接続などの特定の操作をログイン前に実行することができます。PLAP は Windows Vista、Windows 7、Windows 2008 サーバに Start Before Logon 機能を提供します。PLAP は、vpnplap.dll で 32 ビットのオペレーティング システムをサポートし、vpnplap64.dll で 64 ビットのオペレーティング システムをサポートしています。PLAP 機能は、Windows の x86 バージョンおよび x64 バージョンをサポートしています。

注：このセクションでは、VPNGINAはVista以前のプラットフォームのStart Before Logon機能を指し、PLAPはWindows VistaおよびWindows 7システムのStart Before Logon機能を指します。

Vista 以前のシステムでは、Start Before Logon は VPN Graphical Identification and Authentication Dynamic Link Library（vpngina.dll）と呼ばれるコンポーネントを使用して Start Before Logon の機能を提供しています。Windows Vista では、システムに同梱されている Windows PLAP コンポーネントによって、この Windows GINA コンポーネントが置き換えられています。

GINA は、ユーザが Ctrl キーと Alt キーを押した状態で Del キーを押すと起動します。PLAP では、Ctrl キーと Alt キーを押した状態で Del キーを押すとウィンドウが表示され、システムにログインするか、ウィンドウの右下隅にある [Network Connect] ボタンで任意の Network Connections（PLAP コンポーネント）を起動するかを選択できます。

以降の項では、VPNGINA と PLAP SBL の設定と操作手順について説明します。Windows Vista プラットフォームでの SBL 機能（PLAP）の有効化と使用に関する詳細な説明については、「Windows Vista システムでの Start Before Logon（PLAP）の設定」を参照してください。

SBL を有効にするための XML 設定

UseStartBeforeLogon の要素値によって、この機能をオン（true）またはオフ（false）にできます。 プロファイルでこの値を **true** に設定すると、ログイン シーケンスの一部として、追加の処理が発生します。詳細については、Start Before Logon の説明を参照してください。SBL を有効にするため、CiscoAnyConnect.xml ファイルの <UseStartBefore Logon> の値を **true** に設定します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

SBL を無効にするには、同じ値を **false** に設定します。

UserControllable 機能を有効にするには、SBL を有効にするときに次のステートメントを使用します。

```
<UseStartBeforeLogon userControllable="false">true</UseStartBeforeLogon>
```

この属性に関連付けられるユーザ設定は、別の場所に保管されます。

SBL の有効化

ダウンロード時間を最小にするため、AnyConnect クライアントは、サポートする各機能に必要なコア モジュールの（セキュリティ アプライアンスからの）ダウンロードだけを要求します。SBL などの新しい機能を有効にするには、グループ ポリシー WebVPN またはユーザ名 WebVPN コンフィギュレーション モードで **svc modules** コマンドを使用して、モジュール名を指定する必要があります。

```
[no] svc modules {none | value string}
```

SBL のストリング値は **vpngina** です。

次の例では、ネットワーク管理者がグループ ポリシー telecommuters の group-policy 属性モードに切り替え、グループ ポリシーの WebVPN コンフィギュレーション モードに切り替え、文字列 VPNGINA を指定して SBL を有効にします。

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

また、管理者は AnyConnect <profile.xml> ファイル（ <profile.xml> はネットワーク管理者が XML ファイルに割り当てた名前 ）で <UseStartBeforeLogon> ステートメントに **true** が設定されていることを確認する必要があります。次に例を示します。

```
UseStartBeforeLogon UserControllable="false">true
```

Start Before Logon を有効にするには、システムを再起動する必要があります。セキュリティ アプライアンスで、SBL またはその他の追加フィーチャ モジュールを許可することを指定する必要もあります。詳細については、『追加 AnyConnect フィーチャ モジュールの有効化：ASDM（ページ 2-5 ）』または『追加 AnyConnect フィーチャ モジュールの有効化：CLI（ページ 3-4 ）』の説明を参照してください。

Start Before Logon の設定（ CLI ）

このシナリオでは、CLI を使用して XML ファイルを設定する手順を説明します。

1. クライアント PC にプッシュする次のようなプロファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

2. このファイルをセキュリティ アプライアンスのフラッシュにコピーします。

```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```

3. セキュリティ アプライアンスで、WebVPN グローバル セクションにこのプロファイルを使用可能なプロファイルとして追加します。ただし AnyConnect 接続に関するすべての設定が正しいことを前提とします。

```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#
   svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```

4. 使用するグループ ポリシーを編集し、**svc modules** コマンドと **svc profile** コマンドを追加し

ます。

```
hostname(config)# group-policy GroupPolicy internal
hostname(config)# group-policy GroupPolicy attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
hostame(config-group-webvpn)# svc profiles value ReallyNewProfile
```

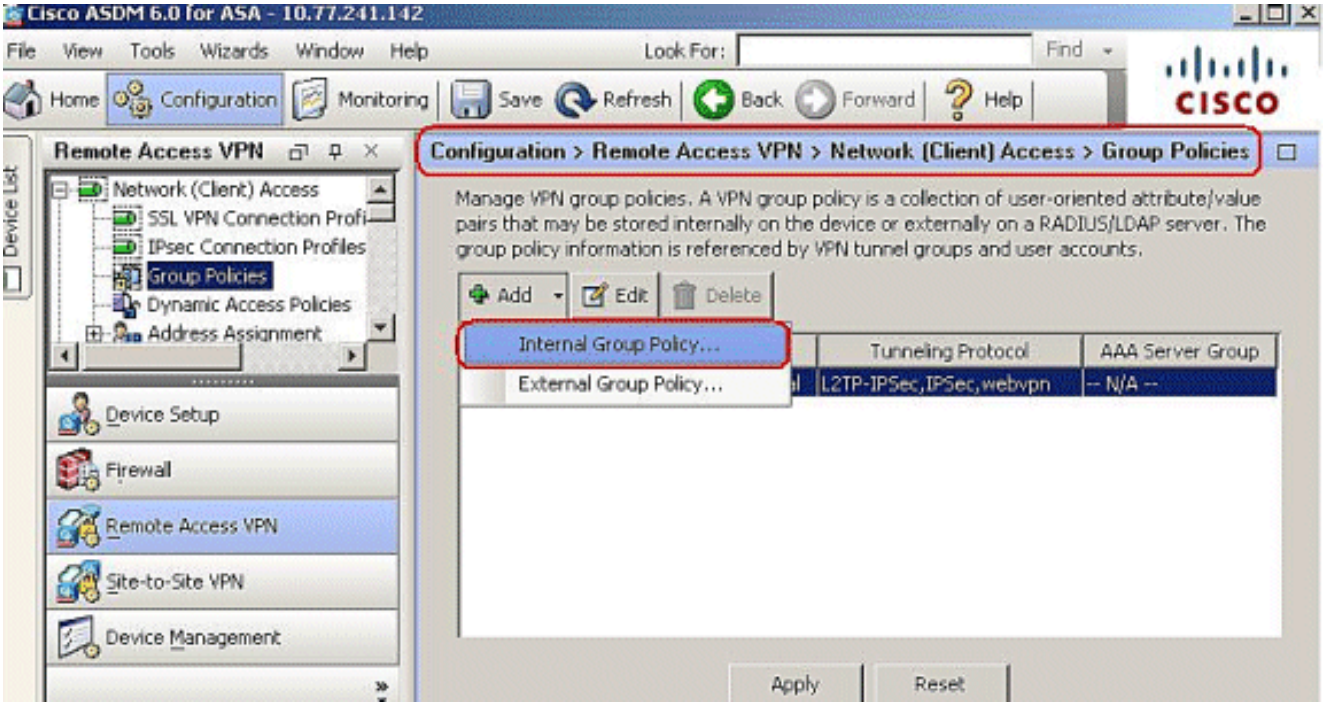
Start Before Logon の設定（ASDM）

ASDM を使用して SBL を設定するには、次の手順を実行します。

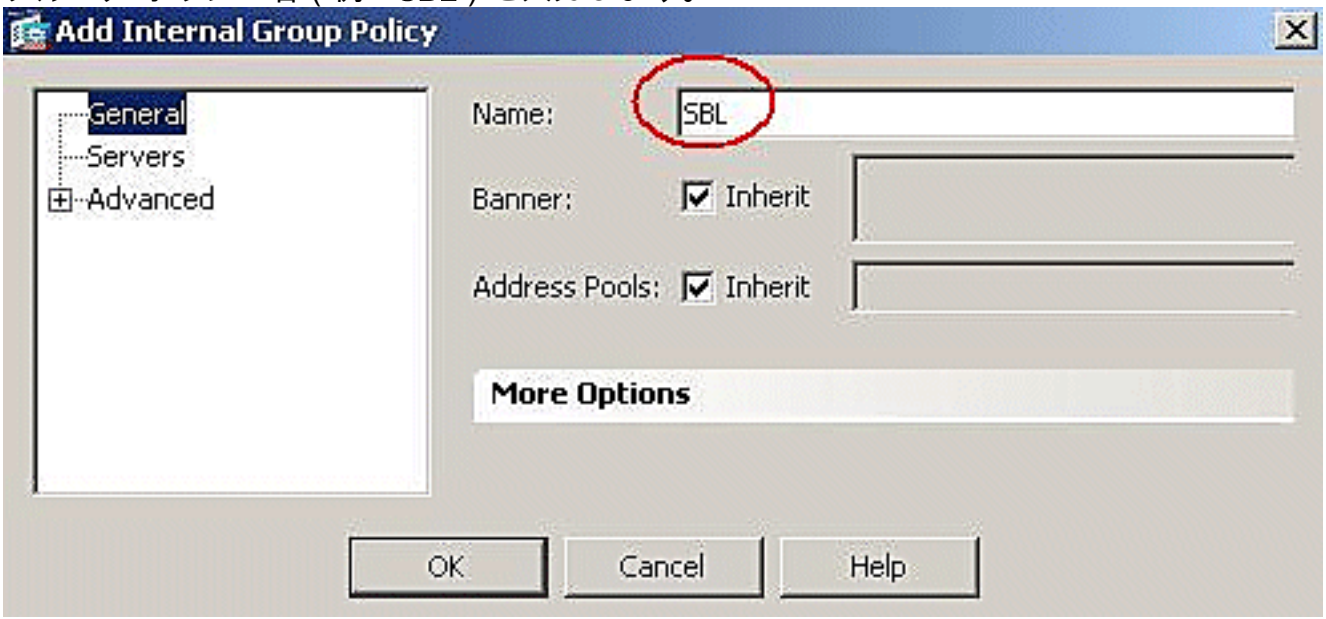
1. クライアント PC にプッシュする次のようなプロファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

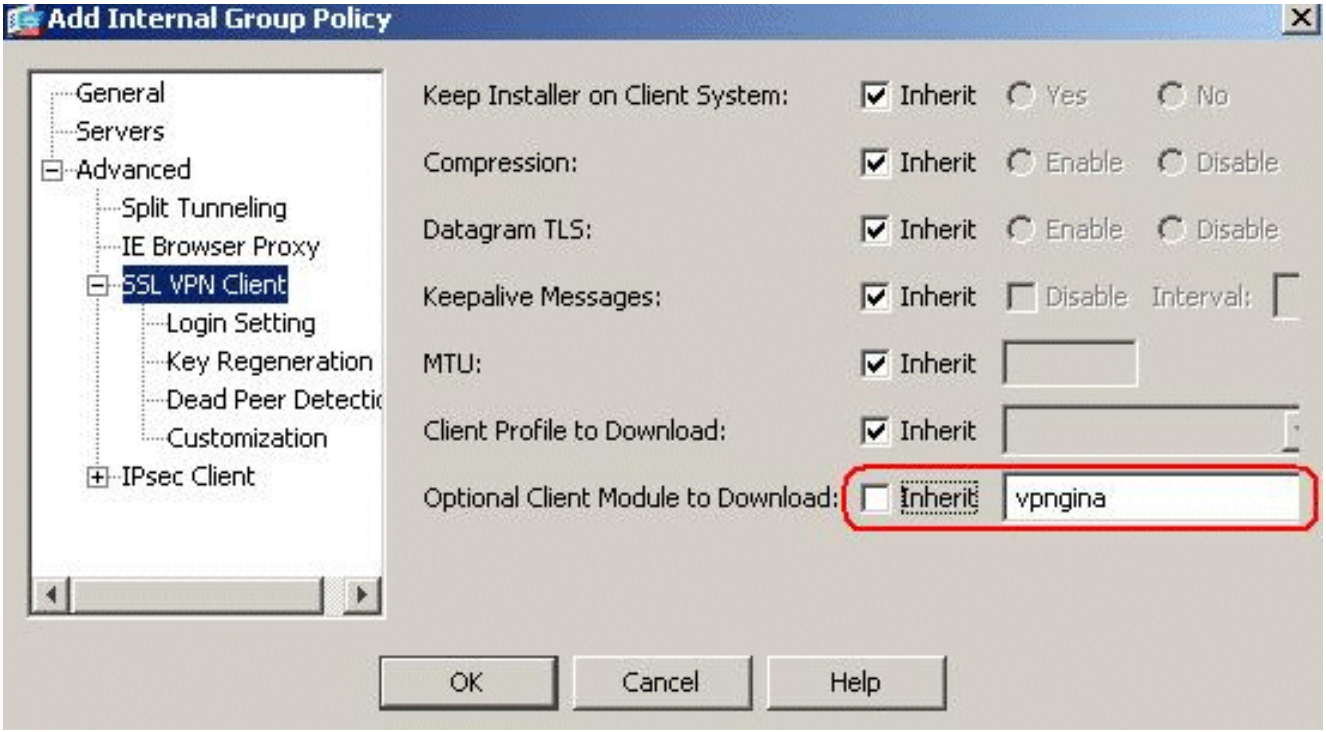
2. このプロファイルを AnyConnectProfile.xml としてローカル コンピュータに保存します。
3. ASDM を起動してホーム ページに移動します。
4. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] に移動し、[Internal Group Policy] をクリックします。



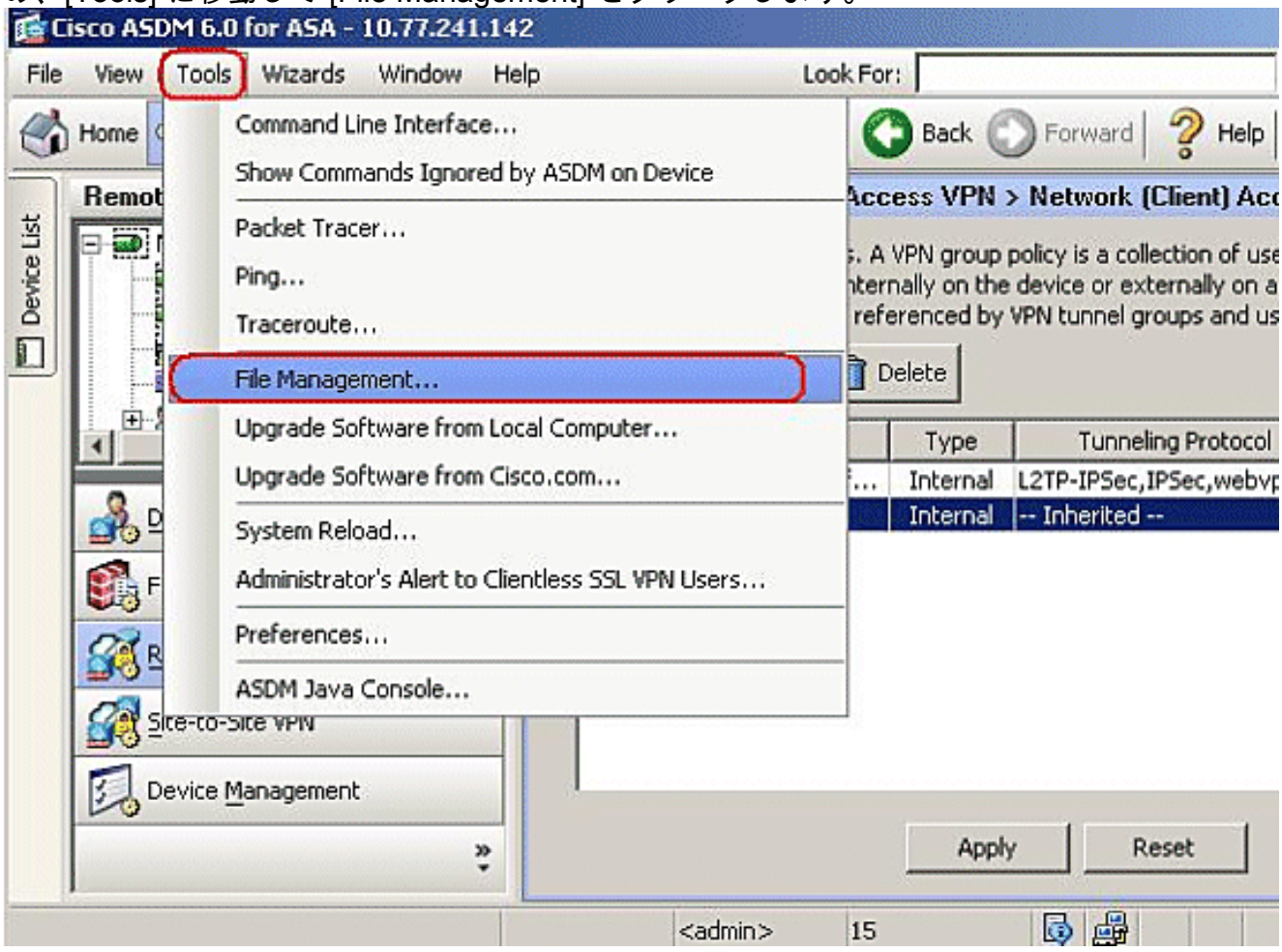
5. グループ ポリシー名（例：**SBL**）を入力します。



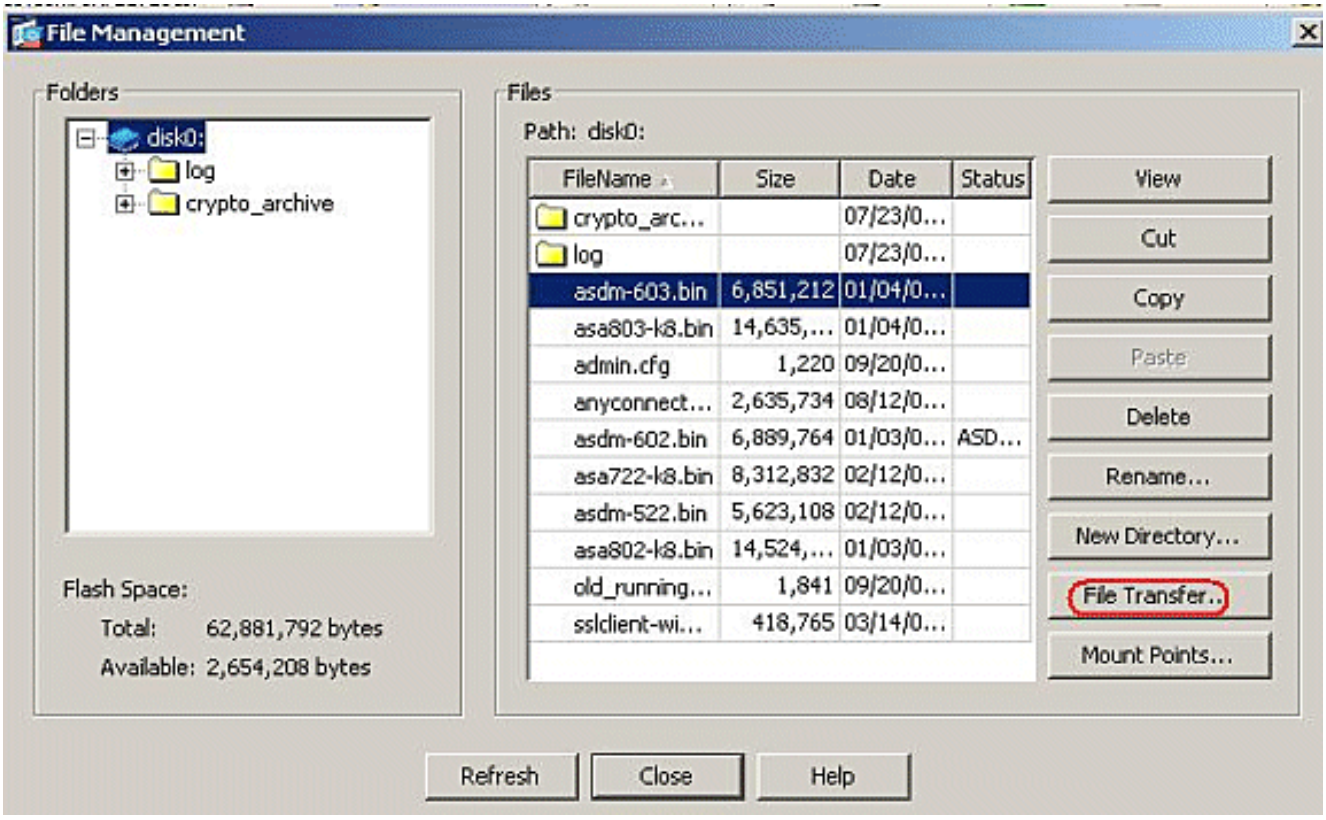
6. [Advanced] > [SSL VPN Client] に移動します。[Optional Client Module to Download] の [Inherit] のチェックマークを外し、ドロップダウン ボックスから [vpngina] を選択します。



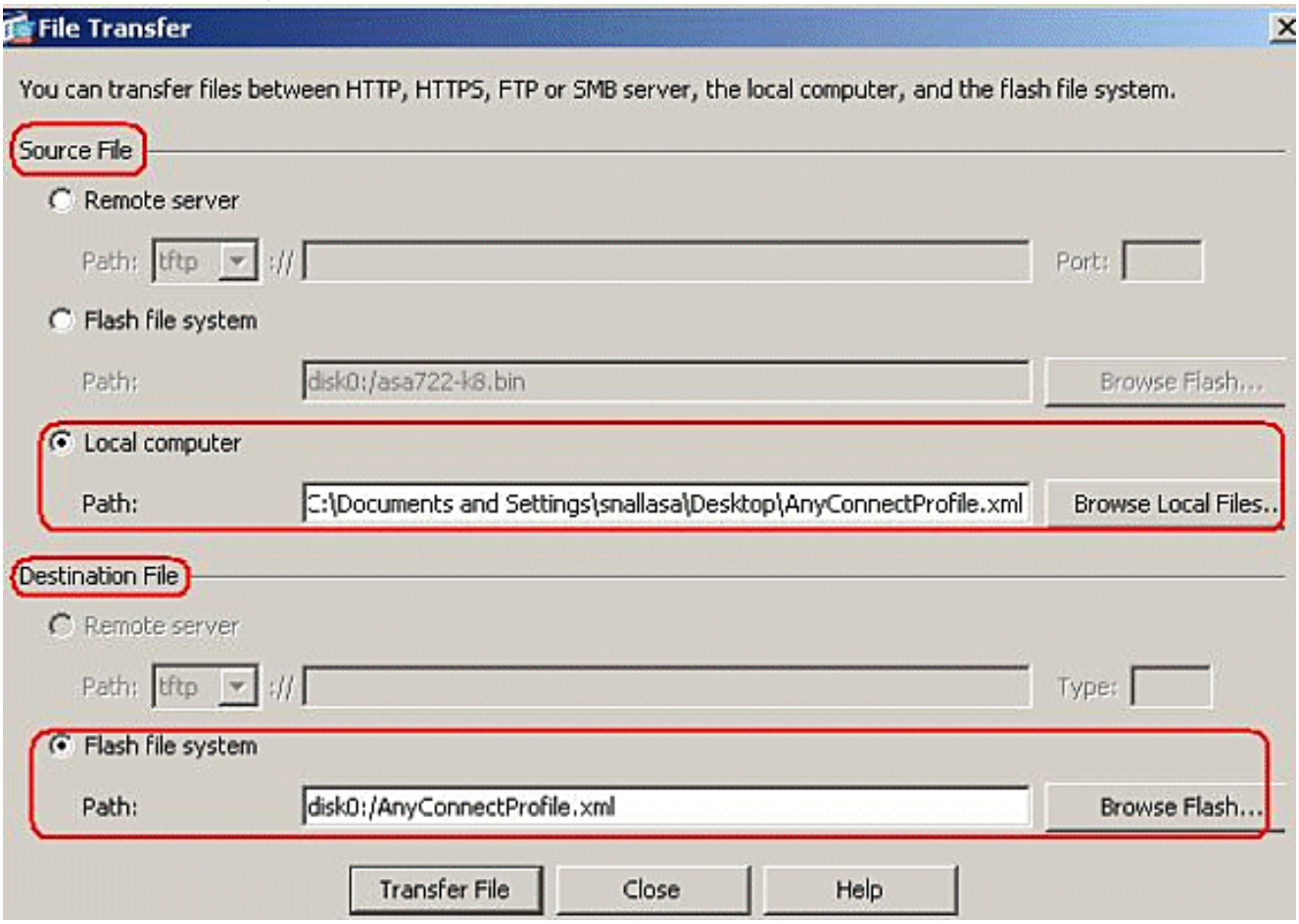
7. プロファイル **AnyConnectProfile.xml** をローカル コンピュータからフラッシュに転送するため、[Tools] に移動して [File Management] をクリックします。



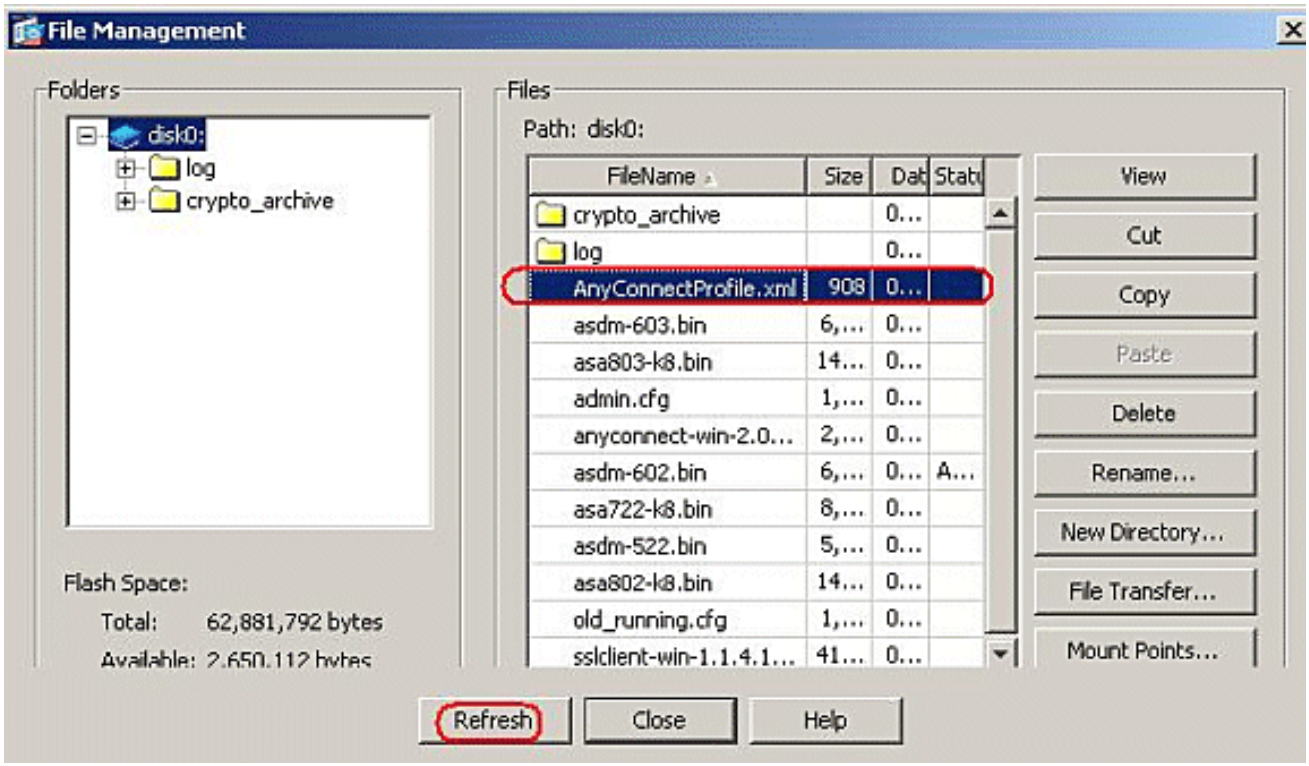
8. [File Transfer] ボタンをクリックします。



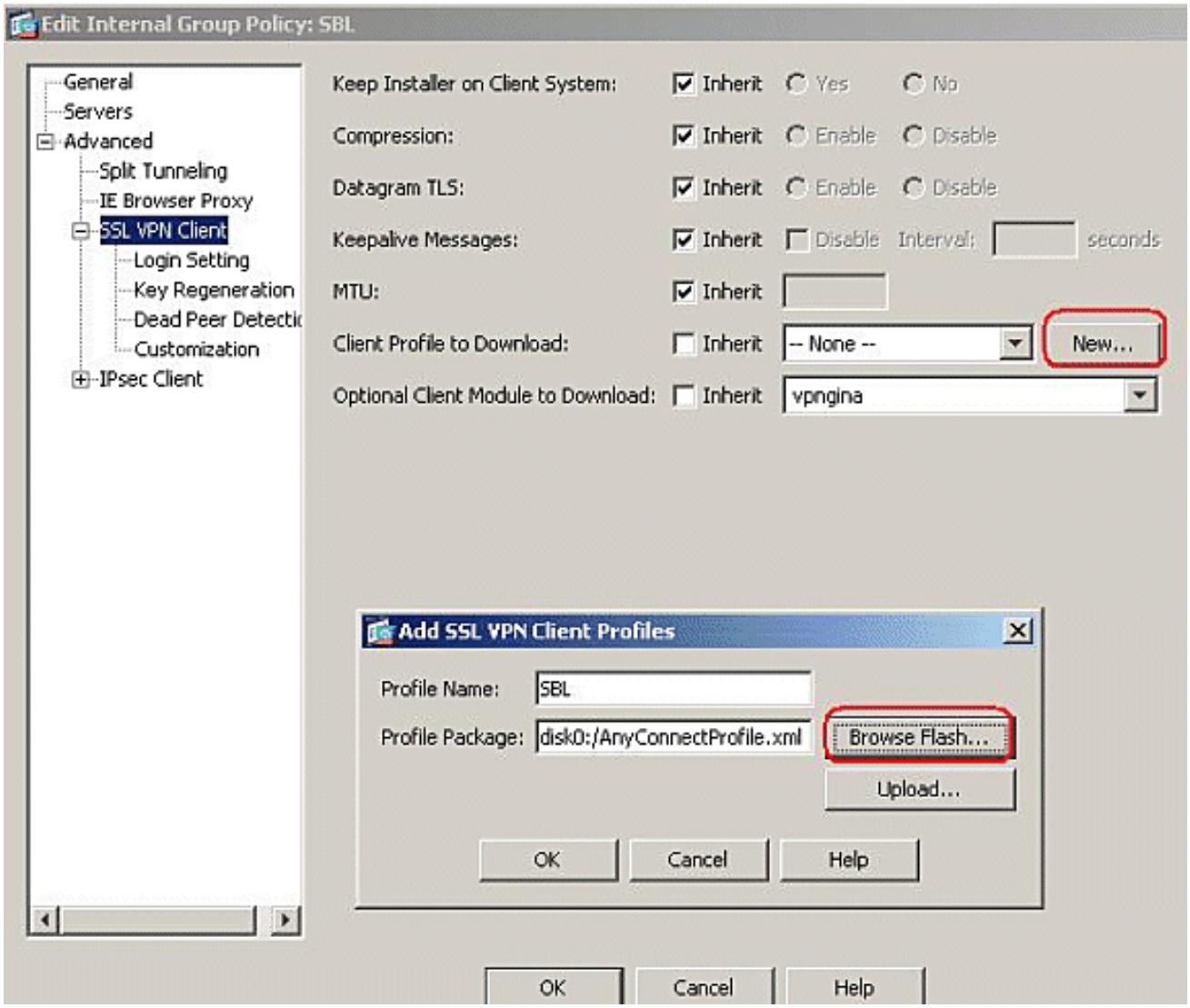
9. プロファイルをローカル コンピュータから ASA フラッシュ メモリに転送するため、要件に基づいて [Source File] 、XML ファイルのパス（ローカル コンピュータ）、[Destination File] のパスを選択します。



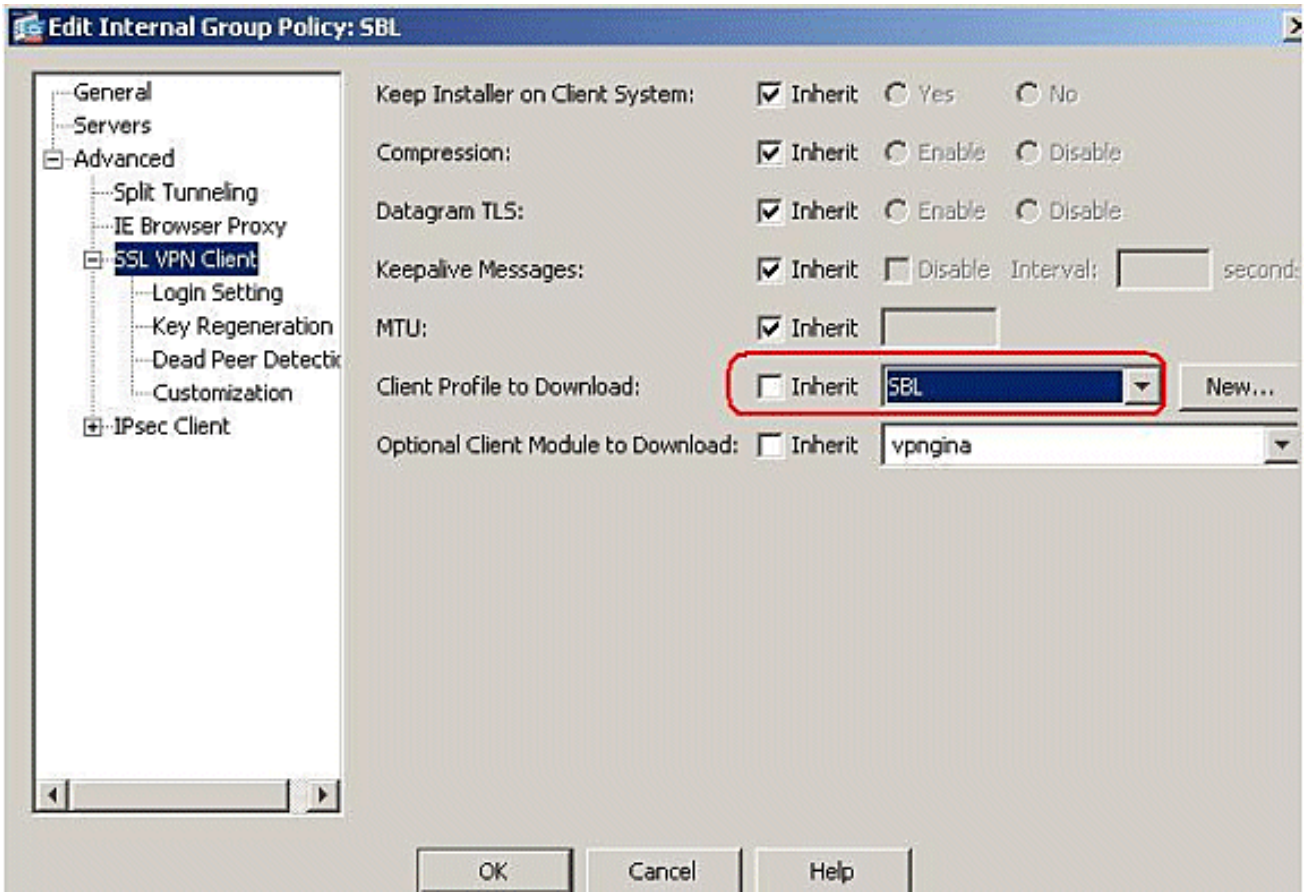
10. 転送が完了したら [Refresh] ボタンをクリックし、プロファイル ファイルがフラッシュ メモリに転送されているかどうかを確認します。



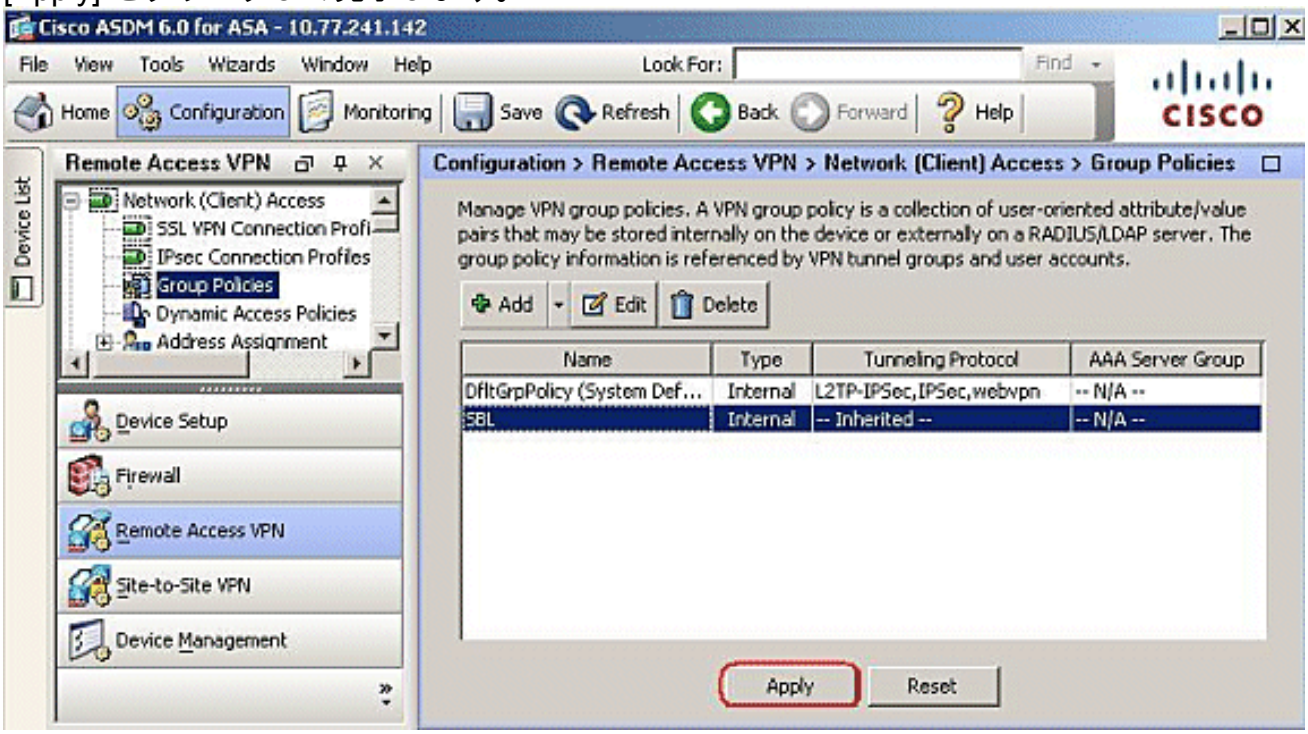
11. プロファイルを内部ポリシー グループ（**SBL**）に割り当てます。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Edit SBL (Internal Group Policy)] > [Advanced] > [SSL VPN Client] > [Client Profile to Download] の順に進み、[New] ボタンをクリックします。[Add SSL VPN Client Profiles] で [Browse] ボタンをクリックし、ASA フラッシュ メモリに保存されているプロファイル（**AnyConnectProfile.xml**）の場所を選択します。プロファイルに**名前**（例：**SBL**）を割り当てます。[OK] をクリックして完了します。



12. [Inherit] チェックボックスのチェックマークを外し、[Client Profile to Download] フィールドで [SBL] を選択します。[OK] をクリックします。



13. [Apply] をクリックして完了します。



マニフェスト ファイルの使用

セキュリティ アプライアンスにアップロードされる AnyConnect パッケージには、VPNManifest.xml というファイルが含まれています。このファイルの内容の例を次に示します。

```
<?xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0">
<file version="2.1.0150" id="VPNCore"
   is_core="yes" type="exe" action="install">
```

```
    <uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
  </file>
  <file version="2.1.0150" id="gina"
    is_core="yes" type="exe" action="install" module="vpngina">
    <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri>
  </file>
</vpn>
```

セキュリティ アプライアンスは、ステップ 1 で説明した設定済みプロファイルを格納しています。また、AnyConnect クライアント、ダウンローダ ユーティリティ、マニフェスト ファイル、さらに他のオプションのモジュールまたはサポート ファイルが含まれる、1 つ以上の AnyConnect パッケージも格納します。

リモート ユーザが WebLaunch または現在のスタンドアロン クライアントを使用してセキュリティ アプライアンスに接続すると、ダウンローダが最初にダウンロードおよび実行されます。ダウンローダはマニフェスト ファイルを使用してリモート ユーザ PC 上にアップグレードする必要がある現行クライアントがあるかどうか、または新規インストールが必要かどうかを確認します。マニフェスト ファイルには、ダウンロードしてインストールが必要なオプションのモジュール（この例では VPNGINA）があるかどうかを示す情報も含まれています。クライアント プロファイルはセキュリティ アプライアンスからもプッシュされます。VPNGINAのインストールは、**svc modules value vpnginaコマンドを使用してアクティブ化します。ステップ4で説明したgroup-policy (webvpn)コマンドモードで設定します**。

ユーザが接続すると、クライアントとプロファイルがユーザ PC に渡され、クライアントと VPNGINA がインストールされ、次回のリブート時、ログオン前に AnyConnect がユーザに対して表示されます。

AnyConnect がインストールされると、サンプル プロファイルがクライアント PC に格納されます（**C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**）。

SBL のトラブルシューティング

SBL で問題が発生した場合は、次の手順を実行します。

1. プロファイルがプッシュされていることを確認します。
2. 古いプロファイルを削除します。ハード ドライブでプロファイルを検索し、その場所を見つけます（*.xml）。
3. [Add/Remove programs] を表示し、AnyConnect と AnyConnect VPNGINA の両方がインストールされていることを確認します。
4. AnyConnect クライアントをアンインストールします。
5. Event Viewer でユーザの AnyConnect ログを消去して再テストします。
6. クライアントを再インストールするために Web をブラウズしてセキュリティ アプライアンスに戻ります。
7. プロファイルも表示されていることを確認します。
8. 1 回リブートします。次のリブートでは、[Start Before Logon] プロンプトが表示されます。
9. AnyConnect イベント ログを .evt フォーマットでシスコに送信します。
10. 次のエラーが表示される場合は、ユーザ プロファイルを削除してデフォルト プロファイルを使用してください。

```
Description: Unable to parse the profile
C:\Documents and Settings\All Users\Application Data\Cisco
\Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml.
Host data not available.
```

問題 1

AnyConnect プロファイルのアップロード中にエラー メッセージ`Error in validating the XML file against the latest schema`この問題の解決方法を次に説明します。

解決策 1

このエラー メッセージが表示される主な原因は、AnyConnect プロファイルの構文または設定の問題です。この問題を解決するには、設定されている AnyConnect プロファイルが、『Cisco AnyConnect VPN Client アドミニストレータ ガイド』の『AnyConnect プロファイルと XML スキーマのサンプル』に記載されているサンプル AnyConnect プロファイルと類似していることを確認します。

関連情報

- Cisco AnyConnect VPN Client アドミニストレータ ガイド、バージョン 2.0
- Creating Logon Scripts - Windows TechNet
- Windows Vista システムでの Start Before Logon (PLAP) の設定
- AnyConnect SSL VPN Client による ASA 8.x VPN アクセスの設定例
- Cisco AnyConnect VPN Client
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- テクニカル サポートとドキュメント – Cisco Systems